

REMARKS

In response to the Office Action mailed September 19, 2008, Applicant respectfully requests reconsideration. To further the prosecution of this application, amendments have been made in the claims, and each of the rejections set forth in the Office Action has been carefully considered and is addressed below. The claims as presented are believed to be in condition for allowance.

Claims 1-39 and 82-94 were previously pending in this application. Claims 1-3, 7-9, 11, 14-16, 20-22, 24, 26-29, 33-35, 37, 39, 82-84, 88-90, 92 and 94 are amended. Claims 5-6, 18-19, 31-32 and 86-87 are canceled. Claims 109-128 are added. As a result, claims 1-4, 7-17, 20-30, 33-39, 82-85, 88-94 and 109-128 are pending for examination, with claims 1, 14, 27 and 82 being independent. No new matter has been added.

Claim Rejections Under 35 U.S.C. §101

Claims 27-39 and 82-94 are rejected under 35 U.S.C. §101 for purportedly being directed to non-statutory subject matter. Specifically, the Office Action contends that the subject matter of independent claims 27 and 82, each of which is directed to a system, may be implemented solely via software, which the Office Action contends is non-statutory.

The assertion that claims that “may be embodied solely via software” are non-statutory is totally unsupported in the Office Action and is traversed. Nevertheless, to further the prosecution of this application, each of claims 27 and 82 is amended to recite the system as comprising at least one processor. In claim 27, the at least one processor is programmed to implement various controllers. In claim 82, the at least one processor is programmed to implement means for capturing, identifying and updating.

As a system comprising at least one processor is clearly statutory under §101, Applicant respectfully requests withdrawal of the rejection of each of claims 27 and 82 under §101 as purportedly being directed to non-statutory subject matter.

Claim Rejections Under 35 U.S.C. §102

Each of independent claims 1, 14, 27 and 82 is rejected under 35 U.S.C. §102(e) as purportedly being anticipated by U.S. Patent No. 7,127,743 to Khanolkar, et al. (“Khanolkar”). Each of claims 1, 14, 27 and 82 is amended herein, and patentably distinguishes over Khanolkar.

A. Brief Overview Of Embodiments Of The Invention

Embodiments of the invention relate generally to monitoring network activity (see Applicant’s specification at, e.g., p. 1, lines 4-5). Many computer systems include one or more mechanisms for reporting on events occurring on the network (p. 1, lines 8-9). For example, many network communications devices (e.g., routers, bridges and switches) produce and transmit a notification for diagnostic and debugging purposes upon processing a network-based event (p. 1, lines 9-11). The notification may describe the event and how it was processed by the device, and may be transmitted on a network protocol such that any device “listening for” the notification on that protocol is informed that the event was processed by the device (p. 1, lines 11-14).

A notification may contain the IP address of the device which produced it, and a code indicating the result of processing the event (p. 1, lines 18-19). The code may indicate, for example, that a requested connection was established, that a processing error occurred, etc. (p. 1, lines 19-21). Because every event processed by every device on a network typically yields at least one notification, collected notifications may become voluminous over time (p. 1, lines 21-22).

A number of conventional systems exist for monitoring and analyzing network activity, including systems which capture notifications and other indications of network activity (p. 1, lines 23-24). These systems typically are designed to detect network events, load information relating to the events to a database, and provide an interface with which a user may analyze the information (p. 1, lines 24-26). The volume of network event notifications can significantly hinder these systems (p. 1, lines 27-28). Specifically, because loading any form of data to a database can inflate the data significantly, the hardware and software needed to store data on network activity, particularly for a large-scale network, can be prohibitively costly (p. 1, lines 28-31). Moreover, as a database grows

in size, the time and processing capacity required to access information stored therein typically progresses geometrically, not linearly (p. 1, line 31 – p. 2, line 1). As a result, many systems try to minimize the amount of data loaded to a database by summarizing, normalizing, or otherwise abridging it (p. 2, lines 1-3). This can become problematic, because while not all network activity data has equal significance, different data may be meaningful at different times, in unpredictable ways (p. 2, lines 3-5). Thus, abridging the data may remove a portion which has great significance to diagnosing a particular network issue (p. 2, lines 5-6).

Some embodiments of the present invention provide techniques for capturing, storing and analyzing observed network activity (p.5, lines 8-11). In some embodiments, rather than loading network activity data to a database that may impose substantial storage overhead and hinder access to the data, an observation record, created from a network event notification, is loaded to a particular one of a plurality of data structures based upon one or more characteristics of the notification (p.5, lines 12-16). Any number of characteristics may trigger a notification record being loaded to a particular data structure (p.5, lines 16-18). For example, a record may be loaded to a particular data structure based on the IP address of the device that issued the notification and/or a time period during which the notification was issued (p.5, lines 18-20). For example, a particular data structure may be loaded with all activity reported by a switch at IP address 192.168.10.3 for a one-minute period starting at 10:03AM (p.5, lines 20-22). Other data structures may be created and loaded with activity data reported by the same device (or other devices) at successive one-minute (or other) increments, such that an ever-expanding series of data structures may be created (p.5, lines 22-24). As a result, a large number of data structures may be created, but a potentially small number of observation records in each data structure may make the data more accessible than it may be in data structures of other types, such as a single large database (p.5, lines 24-27).

Data accessibility may be further improved by providing one or more indices which specify the location of records having certain characteristics (p.5, lines 28-30). For example, an index may indicate a record's location within a data structure, or the data structure itself (p.5, lines 30-32). An index may be created based on any of numerous record characteristics, providing an indication of the location of a record having a certain notification type, originating IP address, destination IP address, and/or any other characteristic (p.5, line 32-p.6, line 3).

The foregoing summary is provided to assist the Examiner in appreciating various aspects of the present invention. However, this summary does not necessarily apply to each independent claim, and the language of each independent claim may differ in material respects from the summary above. Thus, Applicant respectfully requests that careful consideration be given to the language of each independent claim, and that each be addressed on its own merits, without relying on the summary above. In this respect, Applicant does not rely on the foregoing summary to distinguish any of the claims over the prior art, but rather relies only upon the language of the claims and the arguments presented below.

B. Independent Claims 1, 14, 27 and 82

As amended herein, each of independent claims 1, 14, 27 and 82 includes limitations directed to capturing, in a first data structure of a plurality of data structures, a notification provided by a node on a network. The notification has a characteristic, and comprises at least a portion of a transmission by the node describing a networking event. The first data structure is selected among the plurality of data structures to store the notification based at least in part on the characteristic, which comprises an IP address of the node and/or a time period during which the notification occurred. A data element within the notification is identified. An index is updated based on the data element with an indication of a location within the first data structure where the data element is recorded. The data element identifies a notification type for the notification, an originating internet protocol (IP) address for the notification and/or a destination IP address for the notification.

Each of independent claims 1, 14, 27 and 82 patentably distinguishes over Khanolkar, as Khanolkar says nothing about capturing a notification provided by a node on a network in a first data structure selected among a plurality of data structures to store the notification based at least in part on a characteristic of the notification, let alone based on a characteristic comprising an IP address of the node and/or a time period during which the notification occurred. Khanolkar also says nothing regarding updating an index based on a data element within the notification with an indication of where in the first data structure the data element is recorded, and therefore necessarily does not disclose such a data element as comprising a notification type for the notification, an

originating IP address for the notification and/or a destination IP address for the notification.

Khanolkar discloses a system for detecting and monitoring network intrusion events from log data received from network devices (Abstract). Log data is received from various network devices and converted to event objects (col. 2, lines 26-32). Once an event object is created, the information it contains is read to assign a severity level to the object (col. 2, lines 45-46). Objects meeting or exceeding a threshold severity level may be sent to a user or displayed as an intrusion alarm on a user interface in real time (col. 2, lines 47-50). A user may set filters regulating which event objects are sent to the user, based on severity level or other criteria (col. 2, lines 50-52). Event objects are then loaded to a database (col. 7, lines 11-13), which the user may query to discern patterns among various access attempts (col. 4, lines 48-55).

Khanolkar says nothing relating to capturing a notification in a first data structure selected among a plurality of data structures to store the notification based at least in part on a characteristic of the notification. Rather, in the system of Khanolkar, every event object is loaded to a single database 58, depicted in FIG. 2 (col. 7, lines 11-13), such that no selection of a first data structure among a plurality of data structures is performed in the system of Khanolkar.

Khanolkar also says nothing about updating an index with an indication of a location within the first data structure where a data element is recorded. Indeed, an online search of the text of Khanolkar reveals that the word “index” is not used even once. Khanolkar clearly says nothing about updating an index with an indication of a location within a first data structure where a data element comprising a notification type for the notification, an originating IP address for the notification and/or a destination IP address for the notification is located.

In view of the foregoing, each of independent claims 1, 14, 27 and 82 patentably distinguishes over Khanolkar, such that the rejection of each of these claims, and of the claims that depend respectively therefrom, under 35 U.S.C. §102 as purportedly being anticipated by Khanolkar should be withdrawn.

New Claims

Claims 109-128 are presented to further define Applicant's contribution to the art.

Claims 109, 110 and 111 depend from claim 1, which recites a data element as identifying a notification type for a notification, an originating IP address for the notification and/or a destination IP address for the notification. Claim 109 recites that the data element comprises a notification type for the notification, claim 110 recites that the data element comprises an originating IP address for the notification, and claim 111 recites that the data element comprises a destination IP address for the notification. As claims 109-111 depend from claim 1, they are allowable for at least the same reasons as claim 1.

Claims 114-116, 119-121 and 124-126 recite limitations similar to those recited by claims 109-111, respectively. Claims 114-116, 119-121 and 124-126 depend from claims 14, 27 and 82, respectively, and each is allowable for at least the same reasons as its respective base claim.

Claims 112 and 113 depend from claim 1, which recites a notification characteristic as comprising an IP address of the node and/or a time period during which the notification occurred. Claim 112 recites the characteristic as comprising an IP address of the node, and claim 113 recites the characteristic as comprising a time period during which the notification occurred. As claims 112-113 depend from claim 1, they are allowable for at least the same reasons as claim 1.

Claims 117-118, 122-123 and 127-128 recite limitations similar to those recited by claims 112-113, respectively. Claims 117-118, 122-123 and 127-128 depend from claims 14, 27 and 82, respectively, and each is allowable for at least the same reasons as its respective base claim.

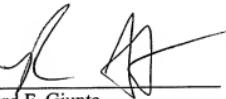
CONCLUSION

A Notice of Allowance is respectfully requested. The Examiner is requested to call the undersigned at the telephone number listed below if this communication does not place the case in condition for allowance.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, the Director is hereby authorized to charge any deficiency or credit any overpayment in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 23/2825, under Docket No. M0929.70003US00.

Dated: December 18, 2008

Respectfully submitted,

By 
Richard F. Giunta
Registration No.: 36,149
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
617.646.8000